Andrew G. Gunem (SBN: 354042)
Raina C. Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com
raina@straussborrelli.com

Attorney for Plaintiff and Proposed Class

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NANCY BALZER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SERVICEAIDE, INC.

Defendant.

Case No. 5:25-cv-4440

CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE AND NEGLIGENCE PER SE**
2. **BREACH OF IMPLIED CONTRACT**
3. **UNJUST ENRICHMENT**
4. **BREACH OF BAILMENT**
5. **INVASION OF PRIVACY**

DEMAND FOR JURY TRIAL

Plaintiff, NANCY BALZER, individually and on behalf of all others similarly situated, brings this Class Action Complaint against SERVICEAIDE, INC. ("ServiceAide" or "Defendant"), and alleges, upon personal knowledge as to her own actions, and upon information and belief as to her counsel's investigations, all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action complaint against Defendant for its failures to

adequately protect the confidential medical information, Personally Identifying Information[1] ("Private Information") and Protected Health Information ("PHI")[2] (collectively, "Private Information") of Catholic Health's patients, resulting in a data security breach between September 19, 2024 and November 5, 2024, in which Plaintiff's and the Class Members' Private Information was exposed including their names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username and password.[3]

2. As a natural and probable result of Defendant's tortious misconduct, Plaintiff and the proposed Class Members have suffered widespread injuries and damages, including but not limited to: invasion of their privacy rights; the unauthorized disclosure of Private Information itself, including on information and belief, publication to the Dark Web; and, she has been forced to expend time and effort to protect herself from identity theft resulting from the Data Breach, including, monitoring her credit reports and account statements, and will be required to do so into

---

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). ServiceAide is a Business Associate, under HIPAA, and some of the data compromised in the Data Breach is "protected health information," subject to HIPAA.

[3] *See SERVICEAIDE, INC Notice of Data Security Event May 5, 2025*, avail. at https://www.serviceaide.com/notices (last acc. May 21, 2025), **attached as Exhibit A.**

the future to mitigate the consequences of the Data Breach.

3. Although Defendant's notice letter[4] offers little detail, what it does say makes clear that Defendant failed to implement and maintain reasonable cybersecurity measures, resulting in the Data Breach. For example, the Data Breach occurred on a portion of the network Defendant refers to as its "information technology support management services to Catholic Health…"[5] strongly implying that Defendant failed to keep that segment of the network updated with the appropriate technologies and safeguards, such as security patches.

4. Moreover, Defendant failed to identify which cybercriminal perpetrated the attack or the materials known to ServiceAide. The absence of information thus likely means that Defendant failed to implement and maintain proper logging, monitoring, and alerting tools such as endpoint detection and response, data loss prevention tools, and centralized alerting.

5. Furthermore, Defendant admits that it discovered the Data Breach on November 15, 2024,[6] and yet waited until May 5, 2025, approximately, over six (6) months before it actually started notifying affected the public and likely thereafter affected individuals, which strongly suggests that Defendant failed to implement and test through appropriate tabletop exercises a reasonable, industry standard cybersecurity incident response plan. The implication is clear because such plans are specifically designed to allow companies to timely investigate and respond to data breaches with a reasonable timeframe. The absence of reasonable and tested response plan further betrays an unreasonable cybersecurity program because a sufficient cybersecurity response plan is a foundational and elemental aspect of any reasonable cybersecurity program.

6. Because of Defendant's failures, approximately 483,126 individuals[7] suffered a

---

[4] *See id.*

[5] *Id.*

[6] *SERVICEAIDE, INC Notice of Data Security Event May 5, 2025*, avail. at https://www.serviceaide.com/notices (last acc. May 21, 2025), **attached as Exhibit A.**

[7] *See* U.S. Dept. of Health and Human Services, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* avail. at

severe invasion of their privacy when Defendant allowed their Private Information to fall into the hands of precisely the individuals their information should be protected from—cybercriminals and identity thieves.

7. Moreover, the 483,126 members of the proposed Class are at a substantially increased risk of identity theft and financial fraud for years to come because Defendant has allowed their Social Security numbers to fall into the hands of identity thieves whose objective it is to use or sell that information for the express purpose of identity theft and financial fraud.

PARTIES

8. Plaintiff Nancy Balzer is a resident and citizen of the State of New York where she intends to remain, with a principal residence in the Town of Tonawanda, New York.

9. Defendant, ServiceAide, Inc., is a corporation organized and existing under the laws of the State of Delaware, with a principal place of business in the State of California at 2445 Augustine Drive, Suite 150, Santa Clara, California 95054.

10. Defendant's Registered Agent for Service of Process is Wai Wong, 2445 Augustine Drive, Suite 150, Santa Clara, California 95054.

JURISDICTION AND VENUE

11. The Court has general subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy is easily more than $5,000,000 and minimal diversity exists. Specifically, the Data Breach affected at least 483,126 people, many of whom may claim at least statutory damages under California law of up to $750 in addition to the further relief sought in the complaint, including reimbursement for out-of-pocket expenses, financial losses from time spent responding to the Data Breach, and the cost of credit monitoring and identity theft protection services. Moreover, minimal diversity exists because Plaintiff is a citizen of New York and Defendant is a citizen of Delaware and/or California.

12. Ther Court has personal jurisdiction over Defendant because it is headquartered in

---

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=E647C1D7465F71D1C8C101ABBFB73D67

this State, and as it transacts substantial business in California, such that it has availed itself to the personal jurisdiction of this State.

13. Venue is proper in this Court because a substantial portion of the events giving rise to this action occurred in this District.

FACTS COMMON TO ALL CLAIMS

A. Defendant and the Data Breach

14. Defendant, ServiceAide, is a California based company, which purports to provide "information technology support management services to Catholic Health," including through its Catholic Health Elasticsearch database.[8]

15. ServiceAide generates annual revenue approximating $50 million.[9]

16. Catholic Health is a "non-profit healthcare system that provides care to Western New Yorkers across a network of hospitals, nursing homes, home care agencies, physician practices, and other community based ministries,"[10] and which generates $1.4 billion per year.[11]

17. Plaintiff and the proposed Class Members provided their Private Information to Defendant, or did so indirectly, through Catholic Health, as a material condition of receiving necessary medial services.

18. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members, including their names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username and

---

[8] *See SERVICEAIDE, INC Notice of Data Security Event May 5, 2025*, avail. at https://www.serviceaide.com/notices (last acc. May 21, 2025), **attached as Exhibit A.**

[9] ZoomInfo, ServiceAide, https://www.zoominfo.com/c/serviceaide-inc/398021107 (last acc. May 21, 2025)

[10] https://www.chsbuffalo.org/about-us/ (last acc. May 21, 2025)

[11] ZoomInfo, Catholic Health, https://www.zoominfo.com/c/catholic-health-system/14797033 (last acc. May 21, 2025).

password.[12]

19. Plaintiff permitted her Private Information to be transmitted to Defendant, and indeed to Catholic Health, solely for the purpose of receiving necessary medical treatment.

20. ServiceAide promises to protect the personal information it collects, stating that "the confidentiality, privacy, and security of personal information within ServiceAide's care is among our highest priorities."[13]

21. Plaintiff's and Class Members' Private Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

22. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

23. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep her Private Information confidential and to protect it from unauthorized access and disclosure.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

25. According to Defendant, "[o]n November 15, 2024, Serviceaide learned that certain information within its Catholic Health Elasticsearch database was inadvertently made publicly available." (the "Data Breach"). [14]

26. Thereafter, Defendant supposedly:

…took steps to secure Catholic Health's Elasticsearch database and initiated an

[12] *See SERVICEAIDE, INC Notice of Data Security Event May 5, 2025,* **Exhibit A.**
[13] *Id.*
[14] *Id.*

> investigation into the nature and scope of the event. The investigation determined that between September 19, 2024 and November 5, 2024, certain patient information was publicly available.[15]

27. However, ServiceAide's notification further stated that, "…the investigation did not identify any evidence that information was copied, but we are unable to rule out ther type of activity. As such, a data review vendor was engaged to conduct a comprehensive and time-intensive review of the potentially impacted data to identify any personal health information contained therein and to whom that information relates. Ther review was recently completed."[16]

28. Based on Defendant's admissions, in the Data Breach, Plaintiff's and the Class Members' Private Information was unauthorizedly disclosed to cybercriminals and compromised, including names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, medical/health information, health insurance information, prescription/treatment information, clinical information, provider names, provider locations, and email/usernames and passwords.[17]

29. Further still, in its Data Breach notices, Defendant encouraged affected victims to monitor their accounts for "unusual" or fraudulent activity, and apprised them of their abilities to place fraud alerts on their credit files and credit freezes on their credit reports.[18]

30. The Data Breach was the direct and proximate result of Defendant's failures to maintain adequate data security protocols, in line with industry standards, as follows hereinafter.

B. Defendant's Data Breach Was Imminently Foreseeable

31. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

32. Data thieves regularly target institutions like Defendant due to the highly sensitive information in her custody. Defendant knew and understood that unprotected Private Information

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*

is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

33. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[19]

34. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

35. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

36. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

37. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

38. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

C. Value of Personally Identifiable Information

39. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20]

[19] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

[20] 17 C.F.R. § 248.201 (2013).

The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

40. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[22]

41. For example, Private Information can be sold at a price ranging from $40 to $200.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[24]

42. Based on the foregoing, the information compromised in the Data Breach is even more significant because it includes Social Security numbers and other government identification, which is significantly difficult if not impossible to change.

43. Ther data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[25]

44. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government

---

[21] *Id.*

[22] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

[23] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[24] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

[25] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

D. Defendant Failed to Comply with FTC Guidelines

45. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

46. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand its network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

---

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

49. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

50. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

E. Defendant Failed to Comply with Industry Standards.

51. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

52. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its

timeline, Defendant failed to follow some or all these industry best practices.

53. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

54. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

55. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

56. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Common Injuries & Damages

57. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to her Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

G. The Data Breach Increases Victims' Risk of Identity Theft.

58. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' Social Security numbers and dates of birth falling into the hands of identity thieves.

59. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the Private Information for the express purpose of conducting financial fraud and identity theft operations.

60. Further, the standard operating procedure for cybercriminals is to use some data, like the Social Security numbers here, to access "fullz packages" of that person to gain access to the full suite of additional Private Information that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[27]

61. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

---

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

62. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

H. Loss of Time to Mitigate Risk of Identity Theft and Fraud

63. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that her Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

64. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers, dates of birth, or other government identification are affected.

65. By spending their time, data breach Plaintiff and the Class are not manufacturing their own harms, but are taking necessary steps at Defendant's direction, especially because the Data Breach included Plaintiff's date of birth and Class Members' Social Security Numbers.

66. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on her accounts; changing passwords and re-securing her own computer networks; and checking her financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

67. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to her good name and credit record."[28]

68. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals her identity), reviewing her credit reports, contacting companies to remove fraudulent charges from her accounts, placing a credit freeze on her credit, and correcting her credit reports.[29]

I. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

69. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

70. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

71. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. Ther is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. Ther is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard her Private Information.

---

[28] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[29] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

J. Plaintiff's Experience

72. Plaintiff provided her Private Information to Defendant, indirectly, through Catholic Health, as a condition of receiving medical treatment from Catholic Health, including at the Kenmore Mercy Hospital location in Kenmore, New York, and other facilities.

73. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system as a result of ServiceAide's relationship with Catholic health.

74. Plaintiff received Defendant's Data Breach notice dated May 9, 2025, informing her that her name, date of birth, medical record number, patient account number, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username and password were disclosed and compromised in the Data Breach.[30]

75. Plaintiff's Private Information was compromised in the Data Breach and stolen by notorious identity thieves who illegally accessed Defendant's network for the specific purpose of targeting the Private Information of Plaintiff and the proposed Class, to be used for criminal and fraudulent purposes.

76. Plaintiff takes reasonable measures to protect her Private Information. She secures all documents containing sensitive medical information, and guards any passwords to online medical records portals. Plaintiff never disseminates her sensitive medical information.

77. As a result of the Data Breach, Plaintiff suffered actual injury in the form of a severe privacy invasion because of her Private Information, including her Date of Birth, falling into the hands of identity thieves, whose mission it is to use that information to perpetrate identity theft and financial fraud.

78. Plaintiff suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of her privacy and because she knows she must now face a substantial increase in identity theft and financial

[30] *See* ServiceAid, *Notice of Security Incident*, May 9, 2025, attached as **Exhibit B.**

fraud attempts for years to come.

79. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name and date of birth, being placed in the hands of criminals whose mission it is to misuse that data.

80. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed because of the Data Breach.

81. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

82. Further, Plaintiff has experienced a dramatic increase in spam communications—one or two new spam calls per day—reflecting the fraudulent misuse of her Private Information disclosed in the Data Breach.

83. In addition to the significantly increased risk of identity theft and financial fraud that Plaintiff must now face because of Defendant's failures, and in addition to the significant invasion of her privacy, Plaintiff has already begun to see the effects of the Data Breach.

CLASS ALLEGATIONS

84. Pursuant to the Federal Rules of Civil Procedure 23(b)(1), 23(b)(3), Plaintiff brings this action on behalf of herself and on behalf of all members of the proposed class defined as:

> **All individuals residing in the United States whose Private Information was unauthorizedly disclosed or compromised in the Data Breach to Defendant's systems between September 19, 2024 and November 5, 2024, including those and to whom Defendant sent an individual notification that they were affected by the Data Breach ("Class").**

85. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as her immediate family members.

86. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

87. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

88. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes 483,126 individuals whose Private Information has been disclosed, and who have been damaged by Defendant's conduct, as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

89. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard her Private Information;

h. Whether Defendant breached her duties to Class Members to safeguard her Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members are entitled to damages;

q. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

90. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class

Members arise from the same operative facts and are based on the same legal theories.

91. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

92. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

93. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating her individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

94. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

95. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send those individuals notification letters.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates the above allegations as if fully set forth herein.

97. Plaintiff and Class Members provided her non-public Private Information to Defendant as a condition of receiving medical treatment from Catholic Health. Defendant received that Private Information from Catholic Health in the capacity as its business associate.

98. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

99. By assuming the responsibility to collect and store their data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

100. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

101. Defendant's duty to use reasonable security measures also arose under the common law, and as informed by the FTC Act, which mandates that Defendant implement reasonable cybersecurity measures.

102. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that her systems and networks, and the personnel responsible for them, adequately protected the Private Information.

103. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

104. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiff and Class Members within Defendant's possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of her Private Information by third parties.

105. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR, data loss prevention tools, and a centralized security event management system;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

106. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

107. Defendant's violation of the FTC Act also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class Members from the harms associated with data breaches.

108. Defendant has admitted that the Private Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

109. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

110. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

111. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

112. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

113. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of her Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

114. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

115. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's decision not to invest enough resources in its cyber defenses amounts to gross negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

116. Plaintiff incorporates the above allegations as if fully set forth herein.

117. Plaintiff and the proposed Class Members transferred her Private Information to Defendant, indirectly or directly, as a material condition of them receiving medical care and treatment from Catholic Health.

118. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members and implicitly agreed to do so.

119. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as a necessary part of receiving healthcare.

120. Defendant, however, failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff

and Class Members provided.

121. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed it to be provided to Defendant.

122. The contract at least implicitly required Defendant to reasonably protect Plaintiff's and Class Members' Private Information.

123. Defendant, however, failed to secure Plaintiff and Class Members' Private Information, as detailed above.

124. Moreover, all contracts include a covenant of good faith and fair dealing in negotiations and in performing the contract, and such good faith requires that Defendant use industry standard, expected, and commercially reasonable means to safeguard the Private Information that force their customers to provide—especially knowing the harm that would result from a data breach should it fail to provide such industry standard protections.

125. If Plaintiff and Class Members knew that Defendant had not reasonably secured her Private Information, they would not have allowed it to be provided to Defendant.

126. Notwithstanding its legal obligations, Defendant failed to implement reasonable cybersecurity measures and thus allowed notorious cybercriminals access to Plaintiff's and Class Members' Private Information.

127. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (Iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the Private Information.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates the above allegations as if fully set forth herein.

129. This cause of action is brought in the alternative to the breach of implied contractual duty claim.

130. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased medical goods and healthcare services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the medical goods and healthcare services that were the subject of the transaction and have their Private Information protected with adequate data security.

131. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

132. The amounts Plaintiff and Class Members paid for medical goods and healthcare services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

133. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards and by Defendant's own representations to Plaintiff and Class Members.

134. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

135. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

136. Had Plaintiff and Class Members knew that Defendant had not reasonably secured

their Private Information, they would not have agreed to Defendant's services.

137. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

138. Plaintiff and Class Members have no adequate remedy at law.

139. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

140. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution, refund, and disgorgement of all inequitable proceeds, profits, benefits, and other compensation obtained by Defendant because of its misconduct and the Data Breach alleged herein, plus attorneys' fees, costs, and interest thereon.

COUNT IV
BREACH OF BAILMENT
(On Behalf of Plaintiff and the Class)

141. Plaintiff incorporates the above allegations as if fully set forth herein.

142. Plaintiff conveyed her Private Information to Defendant lawfully as a condition of her employment with the understanding that Defendant would return or delete her Private Information when it was no longer required or otherwise return it.

143. Defendant accepted the Private Information on the implied understanding that Defendant would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiff's Private Information and act on the Private Information only within the confines of the purposes for which Defendant collected Plaintiff's Private Information.

144. By accepting Plaintiff's data and storing it on its systems, Defendant had exclusive control over the privacy of Plaintiff's data in that Plaintiff had no control over whether Defendant's copy of Plaintiff's Private Information was protected with sufficient safeguards and indeed only Defendant had that control.

145. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendant breached the bailment agreement causing harm to Plaintiff in the form of violations of

her right to privacy and to self-determination of who had/has access to her Private Information, in the form of requiring them to spend her own valuable time responding to Defendant's failures, and in the form of forcing Plaintiff and the Class to face years of substantially increased risk of identity theft and financial fraud.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates the above allegations as if fully set forth herein.

147. By conduct set forth in the preceding paragraphs, Defendant wrongfully intruded upon Plaintiff's and Class Members' seclusion in violation of California law.

148. Plaintiff and Class Members reasonably expected that the personal information they entrusted to Defendant, such as their names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username and passwords would be kept confidential from unauthorized third parties.

149. Defendant unlawfully invaded Plaintiffs' and Class Members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

150. A reasonable person would find it highly offensive that Defendant, having received, collected, and stored Plaintiffs' and Class Members' Private Information and other personal details such as medical facts, failed to protect that information from unauthorized disclosure to third parties.

151. In failing to adequately protect Plaintiff's and Class Members' personal information, Defendant acted knowingly and in reckless disregard of their privacy rights.

152. Defendant also knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's and Class Members' position.

153. Defendant's unlawful invasions of privacy damaged Plaintiffs and Class Members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated, as well as other injuries and damages as set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, NANCY BALZER, individually, and on behalf of all others similarly situated, demands judgment against Defendant, and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

C. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

D. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train her security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess her respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final

judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: May 24, 2025

Respectfully submitted,

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com
raina@straussborrelli.com

J. Gerard Stranch, IV*
Andrew E. Mize*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Telephone: (615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com
gwells@stranchlaw.com

**Pro Hac Vice forthcoming*

Counsel for Plaintiff and the Proposed Class